IN THE CLAIMS

Please cancel claims 3 and 6-8 without prejudice or disclaimer and amend claims 1, 2, 4, and 9 as follows:

1. (Currently amended) A process for ~~restricting unauthorized operations by~~ controlling the applications that a computer user ~~in~~ may run on a multi-user system, comprising the steps of:

automatically using a security executable on the multi-user system in user mode to create a list of authorized ~~operations~~ applications in a database of the multi-user system for ~~said~~ the computer user when the computer user logs on to the multi-user system;

attaching a hook function in user mode to all new ~~processes~~ applications;

employing the hook function whenever a new application is started to send a message to the security executable in user mode, said message including the ~~process~~ ID and path of the new application;

receiving said message from the hook function at the security executable and correlating to said list to determine whether the new application is authorized ~~or not~~;

answering the message by the security executable when the new application is authorized and;

stopping the new application when the new application is not authorized.

2. (Currently amended) A software system for ~~restricting unauthorized operations by~~ controlling the applications that a computer user ~~in~~ may run on a multi-user system, comprising:

a first program module ~~comprising a hook procedure~~ for automatically attaching a hook function to all new ~~processes~~ applications in user mode when the computer user logs on to the multi-user system and for querying an ID of each said new ~~process~~ application; and

a second program module ~~in communication~~ for communicating with said first program module by sending a message with the application ID and the path of the application being examined, said second program module using a security executable on the multi-user system in user mode to build a list of allowed applications in a database of the multi-user system, retrieve the ID of each new ~~process~~ application from said first program module, ~~and~~ terminate each new ~~process~~ application not identified on said list of allowed applications, and answering a message from said first program module when the application is identified on said list of allowed applications.

3. Cancelled.

4. (Currently amended) The software system for ~~restricting unauthorized operations by~~ controlling the applications that a computer user may run according to claim 2, wherein said first program module is attached to said new ~~processes~~ applications by using a system dynamic link library.

5. Cancelled.

6. Cancelled.

7. Cancelled.

8. Cancelled.

9. (Currently amended) A process for ~~restricting unauthorized operations by~~ controlling the applications that computer users ~~in~~ may run on a network environment, comprising the steps of:

using a security executable on the multi-user system in user mode to create and maintain a list of authorized ~~processes~~ applications in a database of the multi-user system and IDs for each computer user when the computer user logs on to the network;

attaching a hook function to all new ~~processes~~ applications;

monitoring all new ~~processes~~ applications that are started with the hook function and determining ~~a process~~ an application ID thereof;

receiving said ~~process~~ application ID from the hook function by the security executable;

determining whether the ~~process~~ application ID of each started ~~process~~ application is on said list;

allowing said ~~process~~ application to continue when its ~~process~~ application ID is on the list; and

terminating said ~~process~~ application when its ~~process~~ application ID is not on the list.